DUMPSARENA

Oracle Cloud Infrastructure 2019 Cloud Operations Associate

Oracle 1z0-1067

Version Demo

Total Demo Questions: 10

Total Premium Questions: 73

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which three statements ate true about Object Storage data security and encryption In Oracle Cloud Infrastructure (OCI)?

A. OCI Key Management is used by default to provide data security.

B. Client-side encryption is managed by the customer.

C. A VPN connection to OCI is required to ensure secure data transfer to an object storage bucket.

D. All traffic to and from Object Storage service is encrypted using TLS.

E. Server side encryption uses per-object keys which are managed by Oracle.

ANSWER: B D E

Explanation:

All data in Object Storage is encrypted at rest by using AES-256. Encryption is on by default and cannot be turned off. Each object is encrypted with its encryption key, and the object encryption keys are encrypted with a master encryption key. In addition, customers can use client-side encryption to encrypt objects with their encryption keys before storing them in Object Storage buckets. An available option for customers is to use the Amazon S3 Compatibility API, along with client-side object encryption support available in AWS SDK for Java.

Data in transit between customer clients (for example, SDKs and CLIs) and Object Storage public endpoints is encrypted with TLS 1.2 by default. FastConnect public peering allows on-premises access to Object Storage to go over a private network, rather than the public internet.

Oracle Cloud Infrastructure Key Management is a managed service the enables you, the customer, to manage and control AES symmetric keys used to encrypt your data-at-rest. Keys are stored in a FIPS 140-2, Level

3- certified, Hardware Security Module (HSM) that is durable and highly available. The Key Management service is integrated with many Oracle Cloud Infrastructure services, including Block Volumes, File Storage, Oracle Container Engine for Kubernetes, and Object Storage.

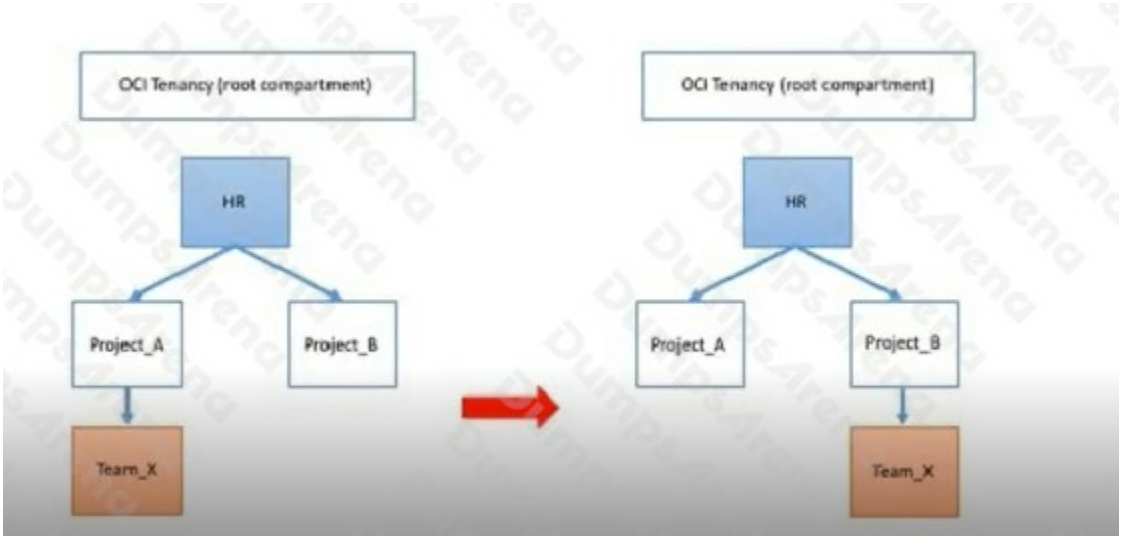
Use the Key Management service if you need to store your Master Encryption Keys in an HSM to meet governance and regulatory compliance requirements or when you want more control over the cryptoperiod of the encryption keys used for your data.

When you store your data with Oracle Cloud Infrastructure Block Volumes, File Storage Service, and Object Storage and don’t use Key Management, your data is protected using encryption keys that are securely stored and controlled by Oracle.

QUESTION NO: 2

Your company has restructured its HR departments. As part of this change, you also need to re-organize compartments within Oracle Cloud Infrastructure (OCI) to align them to the company's new organizational structure. The following change is required:

Comportment Team_x needs to be moved under a new parent compartment, Project_B



The tenancy has the following policies defined for compartments Project_A and Project_B: Policy1 Allow group G1 to manage instance-family in compartment HR:Project_A

Policy2 Allow group G2 to manage instance-family in compartment HR:Project_B Which two statements describe the impacts after the compartment Team_x is moved?

A. Group G2 can now manage instance-families in compartment Project_B compartment Project_A and compartment Team_x

B. Group G1 can now manage instance-families in compartment Project_A but not in compartment Team_x

C. Group G1 can now manage instance-families in compartment project_A,compartment project_B and compartment Team_x

D. Group G2 can now manage instance-families in compartment Project_B and compartment Team_x

E. Group G2 can now manage instance-families in compartment Project_A but not in compartment Team_x

ANSWER: B D

Explanation:

Understanding the Policy Implications When You Move a Compartment

After you move a compartment to a new parent compartment, the access policies of the new parent take effect and the policies of the previous parent no longer apply. Before you move a compartment, ensure that:

- You are aware of the policies that govern access to the compartment in its current position.

- You are aware of the polices in the new parent compartment that will take effect when you move the compartment.

Groups with Permissions in the Current Compartment Lose Access; Groups with Permissions in the Destination Compartment Gain Access

QUESTION NO: 3

You are asked to Implement the disaster recovery (DR) and business continuity requirements for Oracle Cloud Infrastructure (OCI) Block Volumes. Two OCI regions being used: a primary/source region and a DR/destination region.

The requirements are:

• There should be a copy of data in the destination region to use If a region-wide disaster occurs in the source region

• Minimize costs

Which of the following design will help you meet these requirements?

A. Clone block volumes. Copy block volume clones from source region to destination region at regular intervals.

B. Back up block volumes. Use Object Storage lifecycle management to automatically move backup objects to Archive Storage. Copy Archive Storage buckets from source region to destination at regular Intervals.

C. Back up block volumes. Copy block volume backups from source region to destination region at regular intervals.

D. Clone block volumes. Use Object Storage lifecycle management to automatically move clone object Archive Storage. Copy Archive Storage buckets from source region to destination at regular intervals.

ANSWER: C

Explanation:

You can copy block volume backups between regions using the Console, command line interface (CLI), SDKs, or REST APIs. For steps, see Copying a Volume Backup Between Regions. This capability enhances the following scenarios:

Disaster recovery and business continuity: By copying block volume backups to another region at regular intervals, it makes it easier for you to rebuild applications and data in the destination region if a region-wide disaster occurs in the source region.

Migration and expansion: You can easily migrate and expand your applications to another region. You can also enable scheduled cross-region automated backups with user defined policies,

To copy volume backups between regions, you must have permission to read and copy volume backups in the source region, and permission to create volume backups in the destination region.

QUESTION NO: 4

Which three statements are true about Object Storage data security and encryption in Oracle Cloud Infrastructure (OCI)?

A. OCI Key Management is used by default to provide data security.

B. Server side encryption uses per-object keys which are managed by Oracle.

C. All traffic to and from Object Storage service is encrypted using TLS.

D. A VPN connection to OCI is required to ensure security data transfer to an object storage bucket.

E. Client-side encryption is managed by the customer.

ANSWER: B C E

Explanation:

All data in Object Storage is encrypted at rest by using AES-256. Encryption is on by default and cannot be turned off. Each object is encrypted with its encryption key, and the object encryption keys are encrypted with a master encryption key. In addition, customers can use client-side encryption to encrypt objects with their encryption keys before storing them in Object Storage buckets. An available option for customers is to use the Amazon S3 Compatibility API, along with client-side object encryption support available in AWS SDK for Java.

Data in transit between customer clients (for example, SDKs and CLIs) and Object Storage public endpoints is encrypted with TLS 1.2 by default. FastConnect public peering allows on-premises access to Object Storage to go over a private network, rather than the public internet.

Oracle Cloud Infrastructure Key Management is a managed service the enables you, the customer, to manage and control AES symmetric keys used to encrypt your data-at-rest. Keys are stored in a FIPS 140-2, Level

3- certified, Hardware Security Module (HSM) that is durable and highly available. The Key Management service is integrated with many Oracle Cloud Infrastructure services, including Block Volumes, File Storage, Oracle Container Engine for Kubernetes, and Object Storage.

Use the Key Management service if you need to store your Master Encryption Keys in an HSM to meet governance and regulatory compliance requirements or when you want more control over the cryptoperiod of the encryption keys used for your data.

When you store your data with Oracle Cloud Infrastructure Block Volumes, File Storage Service, and Object Storage and don’t use Key Management, your data is protected using encryption keys that are securely stored and controlled by Oracle.

QUESTION NO: 5

You need to set up daily Incremental backups of your database In Oracle Cloud Infrastructure (OCI) Database Service. The backups need to be retained for at least 50 days.

Which of the following method allows you do accomplish this Is an efficient and cost effective manner?

A. Enable automatic backups and choose the preset retention period of 60 days.

B. Enable automatic backups and set the retention period to 50 days.

C. Set up a cron job with OCI Database Service CreateBackuP API call to take periodic full-backups to OCI Object Store. Delete backups older than 50 days.

D. Use Recovery Manager (RMAN) to take backups to an OCI Object Store bucket. Delete backups older than 50 days.

ANSWER: A

Explanation:

When you enable the Automatic Backup feature, the service creates daily incremental backups of the database to Object Storage. The first backup created is a level 0 backup. Then, level 1 backups are created every day until the next weekend. Every weekend, the cycle repeats, starting with a new level 0 backup.

Backup Retention

If you choose to enable automatic backups, you can choose one of the following preset retention periods: 7 days, 15 days, 30 days, 45 days, or 60 days. The system automatically deletes your incremental backups at the end of your chosen retention period.

https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Tasks/backingupOSrman.htm

Also, you can u se Recovery Manager (RMAN) to manage backups of your Bare Metal or Virtual Machine DB system database to your own Object Storage

https://docs.cloud.oracle.com/en-us/iaas/Content/Database/Tasks/backingupOSrman.htm

QUESTION NO: 6

Which two configuration formats does Terraform support? (Choose two.)

A. JSON

B. XML

C. YAML

D. HCL

ANSWER: A D

Explanation:

Terraform configuration files can use either of two formats: Terraform domain-specific language (HashiCorp Configuration Language format [HCL]), which is the recommended approach, or JSON format if the files need to be machine-readable.

QUESTION NO: 7

Several development teams in your company have each been provided with a budget and a dedicated compartment to be used for testing purpose u are asked to help them to control the costs and avoid any overspending.

What should you do?

A. Associate a Budget Tag to each resource with monthly budget amount and use that Information to prepare a weekly report to send to each team.

B. Contact Oracle support and ask them to associate the monthly budget with the Service Limits In every region for which your tenancy is subscribed. The tenancy administrator will receive an alert email from Oracle when the limit Is reached.

C. Associate a Budget Tag to each compartment with the monthly budget amount and set an alert rule to notify the developers' teams when they reached a specific percentage of the budget

D. Configure a Quota for each compartment to prevent provisioning of any bare metal instances.

ANSWER: C

Explanation:

Budgets are set on cost-tracking tags or on compartments (including the root compartment) to track all spending in that cost-tracking tag or for that compartment and its children.

The following concepts are essential to working with budgets:

BUDGET

A monthly threshold you define for your Oracle Cloud Infrastructure spending. Budgets are set on

cost-tracking tags or compartments and track all spending in the cost-tracking tag or compartment and any child compartments. Note: the budget tracks spending in the specified target compartment, but you need to have permissions to manage budgets in the root compartment of the tenancy to create and use budgets.

ALERT

You can define email alerts that get sent out for your budget. You can send a customized email message body with these alerts. Alerts are evaluated every 15 minutes, and can be triggered when your actual or your forecasted spending hits either a percentage of your budget or a specified set amount.

Using Cost-Tracking Tags

You can use cost-tracking tags to help manage costs in your tenancy. Use cost-tracking tags to do any of the following:

- Filter projected costs

- Set budgets

You can only use cost-tracking tag with defined tags. You cannot specify free-form tags as cost-tracking tags.

You can set email alerts on your budgets. You can set alerts that are based on a percentage of your budget or an absolute amount, and on your actual spending or your forecast spending.

QUESTION NO: 8

You are using the Oracle Cloud Infrastructure Command Line Interface to launch a Linux virtual machine.

You enter the following command (with correct values for all parameters):

```
oci compute instance launch --availability-domain "<availability_domain_name>" -t <tenancy_id> -c <compartment_id> --shape
"<shape_name>"   --display-name "<instance_display_name>"   --image-id <image_id> --ssh-authorized-keys-file
"<path_to_authorized_keys_file>" --subnet-id  <subnet_id>
```

The command fails.

Which is NOT a valid parameter in this command?

A. --shape ""

B. -t

C. -c

D. --image-id

E. --subnet-id

ANSWER: B

Explanation:

There's no tenancy_id as a option in oci compute instance launch command. oci compute instance launch [OPTIONS]

--availability-domain [text]

The availability domain of the instance.

--compartment-id, -c [text]

The OCID of the compartment.

--shape [text]

The shape of an instance. The shape determines the number of CPUs, amount of memory, and other resources allocated to the instance.

--display-name [text]

A user-friendly name. Does not have to be unique, and it's changeable. Avoid entering confidential information.

--image-id [text]

The OCID of the image used to boot the instance. This is a shortcut for specifying an image source via the

--source-details complex JSON parameter. If this parameter is provided, you cannot provide the

--source-details or --source-boot-volume-id parameters.

--ssh-authorized-keys-file [filename]

A file containing one or more public SSH keys to be included in the ~/.ssh/authorized_keys file for the default user on the instance.

--subnet-id [text]

The OCID of the subnet where the VNIC attached to this instance will be created. and more options,

https://docs.cloud.oracle.com/en-us/iaas/tools/oci-cli/2.10.1/oci_cli_docs/cmdref/compute/instance/launch.html

QUESTION NO: 9

You want an instance in your compartment to make API calls to other services within Oracle Cloud Infrastructure without storing credentials in a configuration file.

What do you need to do?

A. Create appropriate matching rules in the Dynamic Group to create an Instance Principal

B. No action is required. By default, all VM instances are created with an Instance Principal

C. Instances cannot access services outside their compartment

D. VM instances are treated as users. Create a user and assign the user to that VM instance

ANSWER: A

Explanation:

https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingdynamicgroups.htm

QUESTION NO: 10

Which three must be configured for a load balancer to accept incoming traffic? (Choose three)

A. a back-end server

B. a back end set

C. a listener

D. a security list that is open on a listener port

E. a certificate

ANSWER: A B C

Explanation:

The essential components for load balancing include:

• A load balancer with pre-provisioned bandwidth.

• A backend set with a health check policy. See Managing Backend Sets.

• Backend servers for your backend set. See Managing Backend Servers.

• One or more listeners . See Managing Load Balancer Listeners.

• Load balancer subnet security rules to allow the intended traffic. To learn more about these rules, see Security Rules.

Optionally, youcanassociateyourlistenerswithSSLservercertificatebundlestomanagehowyour system handles SSL traffic. See Managing SSLCertificates.